IBSEC-CSS-M-26
5 June 1970

COMPUTER SECURITY SUBCOMMITTEE

OF THE

UNITED STATES INTELLIGENCE BOARD

SECURITY COMMITTEE

Minutes of Meeting
Held at CIA Headquarters
Langley, Virginia
5 June 1970

1. The Twenty-Sixth meeting of the Computer Security Subcommittee of the United States Intelligence Board Security Committee was held on 5 June 1970 between 0930 and 1245 hours in Room 4E-64, CIA Headquarters Building. In attendance were:

[redacted] STAT
Mr. Alexander S. Chodakowski, State Alternate
[redacted] STAT
Mr. Thomas A. Eccleston, Army Member
Mr. Robert B. Cameron, Navy Member
Capt. Charles L. Bishop, Air Force
[redacted] STAT
Mr. Conrad S. Banner, FBI Alternate
Mr. Raymond J. Brady, AEC Member
[redacted] STAT
Lt. Col. William D. Marsland, Jr., JCS/JCCRG Observer
[redacted] STAT

GROUP I
Excluded from automatic
downgrading and
declassification

[redacted] STAT

Mr. James A. Prell, AEC

[redacted] STAT

2. Briefing on Security Aspects of Compromising Emanations: A significant portion of the instant meeting was taken up with a briefing of members on emanations security. This briefing was provided by Mr. [redacted] of the CIA Communications Security Staff with the assistance of STAT [redacted] defined emanations security as the combination STAT of technical, physical, and personnel control measures needed to prevent the loss of classified information that may be contained in emanations resulting from equipment or systems operations. The briefing and discussion at the meeting centered on the technical aspects of the EMSEC problem.

3. [redacted] outlined that the emanations threat is similar in both STAT the area of communications equipment and other information processing equipment, such as computers and their components. He outlined that a Special Committee on Compromising Emanations (SCOCE) serves under the United States Communications Security Board. The problem of compromising emanations has been referred to for several years by the unclassified codeword TEMPEST. The approach taken to the TEMPEST threat is one of evaluating the combination of equipment vulnerabilities and Soviet capabilities. The emanations may be acoustical, electronic, magnetic, or electromagnetic.

4. For several years a Federal Standard, FS-222, has prescribed requirements for equipment to counter the emanations hazards. These standards are soon to be replaced by Compromising Emanations Laboratory Test Standards (CELTS), due for publication in September 1970 by the Special Committee on Compromising Emanations.

* Attended briefing on Compromising Emanations only

5. [redacted] provided examples of techniques which can be utilized for the exploitation of emanated data, distributed sample analyses of such data, and emphasized that the feasibility of intercepting such material or exploiting such a hazard is dependent on the specific piece of equipment involved and the location in which it is sited. STAT

6. He closed his remarks by calling attention to the fact that most countermeasures for the emanations threat are expensive, as is any program for the testing and evaluation of equipment. He pointed out that within CIA priorities have been established under which high-risk locations are protected and new equipment will be tested as primary objectives; protection of other locations and equipment has a secondary priority.

7. Approval of Minutes: The minutes of the 15 May 1970 Subcommittee meeting (M-25) were approved after a modification of a sentence in paragraph 10 on page 4 as follows: "He also suggested that the assignment of security responsibility noted in the paper be to a single individual or an organizational component."

8. Minimum Requirements for Multi-Level Operation: Discussion was pursued at the instant meeting of the first draft statement of minimum security requirements for multi-level resource-sharing computer systems. The Chairman announced that comments had not been received from all members on the first draft; subsequently, preparation of the second draft had been deferred.

9. Discussion at the instant meeting was coordinated by the Chairman, who had specific items to discuss as proposed by individual member agencies in their separate comments. Among the points discussed were:

a. The Army's proposal that the entire system be secured to the level of the highest material therein;

b. Navy's suggestion that the paper be coordinated with the Deputy Assistant Secretary of Defense for Security Policy;

c. The NSA recommendation to delete the specific examples of compartmented intelligence systems;

d. Clarification of the term "Senior Intelligence Officer";

e. Proposed additional mandatory features, e.g., automatic sign off and storage clear programs;

f. Addition of a section outlining minimum hardware requirements;

g. The suggestion by NSA that the responsibilities of the system security officer be outlined and emphasized.

The Chairman accepted the recommendation of one of the Subcommittee members that a task team work on the redrafting of the paper, this task team being composed of members from CIA, DIA, NSA, and AEC. A meeting of this group was scheduled for 0930 hours on 12 June at CIA. The task team will prepare a second draft for dissemination to members at the next meeting, at which time coordination of the paper may be attempted.

10. Other Business:

a. Mr. Cameron reported that he had received comments from only two member agencies on the latest draft training course outline;

b. The Chairman distributed copies of the attached editorial from the 13 May 1970 issue of Computerworld, entitled "Maximum Security Required," outlining the need for protection of a computer center from intrusion, sabotage, and theft.

11. The next Subcommittee meeting was scheduled for 0930 hours on 19 June 1970 in Room 4E-64 at CIA Headquarters.

[redacted] STAT

Chairman
Computer Security Subcommittee

Attachment

COMPUTERWORLD

May 13, 1970

Editorials

Maximum Security Required

Many companies seem to think of their computer centers as simply modern versions of the old file-storage areas.

This means that the computers and data files effectively have no protection at all.

Old-fashioned file-storage areas had a form of automatic protection. The files were too bulky to cart away easily. And so few people had any interest in going into the filing area that strangers were almost certain to be noticed.

Conditions in a computer center are exactly the opposite. A reel of tape containing a huge block of files can be carried away under someone's coat, copied within a short time, and returned unnoticed. And computer centers attract so many visitors and employees that no one pays much attention to people wandering around the installation.

Because computer centers are so valuable – and so vulnerable – they should be treated like bank vaults, not file-storage areas.

They should be locked from the outside, and no one should be admitted without first showing proper authorization.

If management considers the center a showplace, one or more walls of the center should be made of bullet-proof glass. Visitors should be kept on the outside.

As further protection, duplicate copies of all software and key files should be kept under lock somewhere removed from the center, so that if the worst happens, the installation can recover easily.

Such precautions would not only protect the center from minor problems but would also prevent incidents such as the one at Sir George Williams University [CW, April 29].